424 Rec'd PCT/PTO 26 MAY 2000

FORM PTO-1390 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE TRANSMITTAL LETTER TO THE UNITED STATES DESIGNED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		ATTORNEY'S DOCKET NO. PHD 99-096 U.S. Application No. (if known, see 37 CFR 1.5) 09/555303
INTERNATIONAL APPLICATION NO PCT/EP99/07025	INTERNATIONAL FILING DATE SEPTEMBER 21, 1999	PRIORITY DATE CLAIMED SEPTEMBER 30, 1998 and August 5, 1999

TITLE OF INVENTION
DATA PROCESSING DEVICE AND OPERATING METHOD FOR PREVENTING A DIFFERENTIAL CURRENT CONSUMPTION ANALYSIS

APPLICANT(S) FOR DO/EO/US
MARKUS FEUSER

Applicant(s) herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.

2. [ ] This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.

3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).

4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. [X] A copy of the International Application as filed (35 U.S.C. 371 (c)(2))
   a. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).

6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2))

7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [X] have not been made and will not be made.

8. [ ] A translation of the amendment to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).

9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. Below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.

12. [X] An assignment document for recording. A separate cover sheet is compliance with 37 C.F.R. 3.28 and 3.31 is included.

13. [X] A FIRST preliminary amendment.
    [ ] A SECOND OR SUBSEQUENT preliminary amendment.

14. [ ] A substitute specification.

15. [ ] A change of power of attorney and/or address letter.

16. [X] Other items or information:
    Charge Authorization

"EXPRESS MAIL" MAILING LABEL NUMBER EL297131917US

DATE OF DEPOSIT MAY 26, 2000

I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 CFR 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO THE COMMISSIONER OF PATENTS AND TRADEMARKS, WASHINGTON, D.C. 20231.

Josephine Cangelosi

(TYPED OR PRINTED NAME OF PERSON MAILING PAPER OR FEE)

Josephine Cangelosi

(SIGNATURE OF PERSON MAILING PAPER OR FEE)

S:\pw\mu24pwq0.cn0

U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5) 09/555303	INTERNATIONAL APPLICATION NO. PCT /EP99/07025	ATTORNEY'S DOCKET NUMBER PHD 99-096

17 [x] The following fees are submitted:

BASIC NATIONAL FEE (37 C.F.R. 1.492(A)(1)-(5)):

		CALCULATIONS (PTO USE ONLY)
Search Report has been prepared by the EPO or JPO	$940.00	
International preliminary-examination fee paid to USPTO (37 C.F.R. 1.482)	$720.00	
No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2)	$760.00	
Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2)) paid to USPTO	$970.00	
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)	$ 96.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =		$970.00

Surcharge of $130.00 for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).				$	
CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE	
Total Claims	11	- 20 =		X $ 18.00	$
Independent claims	2	- 3 =		X $ 78.00	$
MULTIPLE DEPENDENT CLAIMS (if applicable)				+ $260.00	$
TOTAL OF ABOVE CALCULATIONS =					$970.00
Reductions by 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 C.F.R. 1.9, 1.27, 1.28)					$
SUBTOTAL =					$970.00
Processing fee of $130.00 for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(f)). +					$
TOTAL NATIONAL FEE =					$
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28,3.31). $40.00 per property +					$ 40.00
TOTAL FEES ENCLOSED =					$1,010.00
				Amount to be Refunded	$
				Charged	$

a. [ ] A check in the amount $_____ to cover the above fees is enclosed.

b. [X] Please charge my Deposit Account No. 14-1270 in the amount of $ 1,010.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fee, with the exception of the Base Issue Fee, which may be required, or credit any overpayment to Deposit Account No. 14-1270. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Corporate Patent Counsel
Philips Electronics North America Corporation
580 White Plains Road
Tarrytown, NY 10591

(SIGNATURE)

Daniel J. Piotrowski
(NAME)

42,079
(REGISTRATION NUMBER)

DATE OF MAILING:

5/26/00

S:\pw\mu24pwq0.cn0

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

MARKUS FEUSER

Atty. Docket

PHD 99-096

Serial No.

Filed: Concurrently

DATA PROCESSING DEVICE AND OPERATING METHOD FOR PREVENTING A DIFFERENTIAL CURRENT CONSUMPTION ANALYSIS

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to calculation of the filing fee and examination, please amend the above-identified application as follows:

IN THE CLAIMS

Please amend claims 4, 5, 9, 10 and 11 as follows:

Claim 4, line 1, change "one of the Claims 2 or 3" to --Claim 3--.

Claim 5, line 1, change "one of the Claims 2 to 4" to --Claim 4--.

Claim 9, line 1, change "one of the Claims 7 or 8" to --Claim 8--.

Claim 10, line 1, change "one of the Claims 7 to 9" to --Claim 9--.

Claim 11, line 1, change "one of the Claims 7 to 10" to --Claim 10--.

REMARKS

The claims are amended to remove multiple dependency without change in scope.

Entry of the Amendment is respectfully requested.

Respectfully submitted,

By _____
Daniel J. Piotrowski, Reg. 42,079
Attorney
(914) 333-9624

Data processing device and operating method for preventing a differential current consumption analysis.

The invention relates to a method of operating a data processing device, notably a chip card, which includes an integrated circuit which executes useful arithmetic operations, notably cryptographic operations, in dependence on a first clock signal as disclosed in the introductory part of Claim 1. The invention also relates to a data processing device, notably a chip card, which is specifically intended to carry out the method and includes an integrated circuit which executes useful arithmetic operations, notably cryptographic operations, in dependence on a first clock signal as disclosed in the introductory part of Claim 6.

In many data processing apparatus provided with an integrated circuit, for example, cryptographic operations are carried out so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried out by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a chip card or an IC card. Data or intermediate results used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

The arithmetic operations performed by the integrated circuit, for example in order to calculate cryptographic algorithms, involve the formation of logic combinations of operands or intermediate results. Depending on the technology used, such operations, notably the loading of empty or previously erased storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of the current consumption occurs when the value of a bit storage cell changes, i.e. when its value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the Hamming weight of the operand (= number of bits having the value "1") written into the empty register. Analysis of this current variation could thus enable extraction of information

concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. When several current measurements are performed on the data processing apparatus, adequate information could be extracted, for example in the case of very small signal variations. On the other hand, a plurality of current measurements could also enable a possibly required differentiation. This type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus. "Differential Power Analysis" thus enables the extraction of additional internal information of an integrated circuit beyond pure functionality.

US 4,813,024 discloses an integrated circuit for the storage and processing of secret data wherein a memory includes a simulation storage cell whose current consumption is identical to that of a storage cell which has not been programmed thus far. Fluctuations in the current and the voltage are thus substantially but not completely eliminated. This system is also very complex and expensive.

EP 0 482 975 B1 discloses a memory card which includes a microcircuit and at least one memory which is connected to a data processing member, the data processing member being controlled by a data signal from outside the card and delivering a command transmission signal in response to said data signal at a given instant, said command transmission signal being delayed by a predetermined period of time (T) relative to the reception of the data signal, the period of time (T) being selected so as to be variable in time on a random basis in order to enhance the security. Thus, a period of time elapsing between the reception of an external signal and a response is subject to a random generator and is not suitable for evaluation for the purpose of extraction of secret data. Crypto analysis on the basis of a current variation during the writing of the memory or the execution of arithmetic operations, however, cannot be precluded by such a system.

EP 0 507 669 A1 discloses a card for electronic payment, i.e. a so-called paycard, in which each pay unit comprises a plurality of bits instead of only a single bit, the additional bits numbering the pay units in a random series and being derived from a random number series. This random number series is available to sales outlets accepting a paycard. However, this system again is not capable of precluding crypto analysis on the basis of a current variation occurring during the writing of the memory or the execution of arithmetic operations.

FR 2 693 014 B1 describes a device for evaluating chip cards, for example a public telephone, which determines, by way of a capacitance measurement, whether external apparatus is connected to an inserted chip card.

It is an object of the present invention to provide an improved method and an improved data processing device of the kind set forth which eliminate the described drawbacks and offer effective protection against "Differential Power Analysis".

This object is achieved by means of a method of the kind set forth which is characterized as disclosed in Claim 1, and by means of a data processing device of the kind set forth which is characterized as disclosed in Claim 6.

To this end, in conformity with the method of the kind set forth according to the invention a second clock signal is derived from the first clock signal under random control so as to be applied to the integrated circuit instead of the first clock signal while distances between clock edges of the second clock signal vary at random in time.

This offers the advantage that the execution in time of useful arithmetic operations is distorted independently of data processed in the data processing device, so that a share of the power consumption of the integrated circuit which is characteristic of a useful arithmetic operation or operations is disguised and can no longer be analyzed by means of "Differential Power Analysis".

Preferred further versions of the method are described in the Claims 2 to 5.

In order to disguise a characteristic share of the current consumption of the integrated circuit which is due to calculations or useful operations of the integrated circuit even further, the integrated circuit is switched to different modes of operation under random control.

In order to prevent reproducibility of the characteristic share of the current consumption which is due to identical useful operations, the different modes of operation involve at least two calculation methods which produce an identical result while using different approaches.

In order to disguise the type and time of the useful arithmetic operations even further, the different modes of operation include at least one "dummy" mode in which the integrated circuit executes dummy arithmetic operations instead of useful operations, said dummy operations processing predetermined input data or random input data, the result being rejected and not taken up in the results or input data for the useful arithmetic operations.

Optionally, there is provided an additional mode of operation "deactivated" in which the integrated circuit does not execute arithmetic operations.

A data processing device of the kind set forth according to the invention is provided with a clock control unit which is connected to the integrated circuit as well as with a random generator which is connected to the clock control unit, the clock control unit being constructed in such a manner that it generates a second clock signal in dependence on the random generator and the first clock signal, which second clock signal varies at random and controls the integrated circuit.

This offers the advantage that the execution in time of useful arithmetic operations is distorted independently of data processed in the data processing device, so that a share of the current consumption of the integrated circuit which is characteristic of the useful arithmetic operations is disguised and can no longer be analyzed by way of "Differential Power Analysis".

Further preferred embodiments of the data processing device are described in the Claims 7 to 10.

The invention will be described in detail hereinafter with reference to the accompanying drawings. Therein

Fig. 1 shows a block diagram of a preferred embodiment of a data processing device according to the invention, and

Fig. 2 graphically illustrates various signals generated and used in the data processing device.

Fig. 1 shows a preferred embodiment of a data processing device 100 according to the invention which includes an integrated circuit 10, a random generator 12 and a clock control unit 14. The integrated circuit 10 carries out useful arithmetic operations to be described hereinafter. Useful arithmetic operations are arithmetic operations which process input data in a desired manner and produce a desired result or intermediate result. An example in this respect is a predetermined arithmetic method involving cryptographic operations and executed in dedicated crypto processors. Such a predetermined arithmetic method will be referred to as the method 1 or the first mode of operation hereinafter.

Fig. 2 shows, as a function of time t, various signals which are generated in the data processing unit 100 and are plotted on a horizontal axis 16. The reference numeral 18 denotes a signal $TAKT_1$ which controls the clock control unit 14 via a lead 19. The reference numeral 20 denotes a signal $TAKT_2$ which is generated by the clock control unit 14 and is applied to the integrated circuit 10 via a lead 21. The reference numeral 22 denotes a signal DUMMY whereas the reference numeral 24 denotes a signal DEAKT and the reference numeral 26 denotes a signal ALT, said signals being applied, via control leads 28, from the clock control unit 14 to the integrated circuit 10 in order to control the latter. An additional line 29 shows the instantaneous mode of operation of the integrated circuit 10 under the control of the clock control unit 14. The reference numeral 30 denotes a mode of operation "method 1", whereas the reference numeral 32 denotes a mode of operation "dummy", the reference 34 denotes a mode of operation "method 2" and the reference numeral 36 denotes a mode of operation "deactivated". These modes of operation 30, 32, 34 and 36 and their functions will be described in detail hereinafter.

According to an article "Differential Power Analysis" published by Paul Kocher on the Internet under http://www.cryptography.com/dpa not only the input/output signals are analyzed but also a current consumption I_a or voltage drops ΔU_a of a supply voltage U_a of the integrated circuit. The success of this method of analysis is dependent on whether a number N_A of analog ($I_a(t)$ or $\Delta U_a(t)$) signal variations $S(k,t)$ in time can be measured with $k = \{1,...,N_A\}$ different operands in such a manner that it is possible to form a sum of the form:

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k).S(k,t)$$

with the coefficients p(ik), where $i = \{0,1,2,...\}$. When different signal variations $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$ ... are observed at the same instant $t = t_1$, differential power analysis can be successful only if the integrated circuit executes the same arithmetic operation with different operands $k = \{1,...,N_A\}$ at that instant, i.e. it must be possible to make the signal variations S(k,t) register exactly. This holds not only for the calculation itself, but also for the input and output of data.

The invention prevents such "registration" in that the integrated circuit 10 is controlled by the random controlled clock control unit 14. Moreover, the integrated circuit not only has the mode of operation "method 1" 30, but also the mode of operation "dummy"

32 in which dummy calculation operations to be described hereinafter are executed, the mode of operation "deactivated" 36 in which the integrated circuit 10 does not execute arithmetic operations and results or intermediate results formed thus far are possibly stored, and the mode of operation "method 2" 34 in which the useful arithmetic operations of the "method 1" 30 are executed by means of an alternative method; the result thereof is not different from that of the first mode of operation "method 1" 30 but is merely calculated in a different way, so that in comparison with the "method 1" 30 the "method 2" 34 involves a different variation of the input current I_a or different voltage variations ΔU_a of the integrated circuit 10 for the same operands k.

Dummy arithmetic operations are arithmetic operations which act on predetermined input data or input data selected at random, the result being rejected and not being taken up in the results or the input data for the useful arithmetic operations.

The clock control unit 14 is controlled, via the lead 19, by the signal $TAKT_1$ 18 as well as by the random generator 12 via the lead 38. The clock control unit 14 generates a random clock signal $TAKT_2$ 20 from $TAKT_1$ 18 and the input from the lead 38, which clock signal $TAKT_2$ 20 distorts the time axis 16 in S(k,t) independently from the data calculated in the integrated circuit 10. This makes it impossible to perform the above-mentioned summing with the desired result for the differential power analysis.

Furthermore, from one clock edge until a later clock edge the control signals DUMMY 22, DEAKT 24 and ALT 26 are set on the control leads 28, in dependence on the random generator, in the manner shown in Fig.2. During the signal DUMMY 22 the integrated circuit 10 operates in the mode "dummy" 32; in the presence of the signal DEAKT 24 the integrated circuit 10 operates in the mode "deactivated" 36, whereas in the presence of the signal ALT 26 the integrated circuit 10 operates in the mode "method 2" 34, whereas if no signal is present on the control leads 28, the integrated circuit 10 operates in the mode "method 1" 30 as is demonstrated by the line 29 in Fig. 2 which illustrates the modes of operation.

The mode of operation "dummy" 32 disguises the actual calculation S(k,t). It is possible to provide several, different modes of operation "dummy n" with corresponding, different signals "DUMMY n". It is particularly advantageous when the instant and duration of the dummy signals are not determined by the integrated circuit 10 to be protected itself, but by the external devices consisting of the random generator 12 and the clock control unit 14. In the mode of operation "deactivated" 36, the time axis 16 is additionally distorted further so that the above-mentioned formation of the sum for the "Differential Power

Analysis" is additionally impeded or made impossible. In the mode of operation "method 2" 34 the calculation is further disguised, so that the calculation S(k,t) is difficult to identify. If desired, further, different modes of operation with a different calculation approach "method n" are provided and also associated signals "ALT n".

Summarizing it can be said that according to the invention a characteristic share of the current consumption of the integrated circuit 10 is not eliminated but disguised. To this end, different methods of disguise are flexibly combined by means of the clock control unit 14. To some extent dummy signals are generated by dummy calculations which cannot be recognized as such from the outside, because they are generated on a random basis.

CLAIMS:

1. A method of operating a data processing device (100), notably a chip card, which includes an integrated circuit (10) which executes useful arithmetic operations, notably cryptographic operations, in dependence on a first clock signal, characterized in that a second clock signal is derived from the first clock signal under random control so as to be applied to the integrated circuit (10) instead of the first clock signal while distances between clock edges of the second clock signal vary at random in time.

2. A method as claimed in Claim 1, characterized in that the integrated circuit (10) is switched to different modes of operation under random control.

3. A method as claimed in Claim 2, characterized in that the various modes of operation include at least two calculation methods which produce an identical result while using different arithmetical approaches.

4. A method as claimed in one of the Claims 2 or 3, characterized in that the various modes of operation include at least one mode of operation "dummy" (32) in which the integrated circuit (10) does not execute useful operations but dummy arithmetic operations which act on predetermined or random input data, the result being rejected and not taken up in the results or input data for the useful arithmetic operations.

5. A method as claimed in one of the Claims 2 to 4, characterized in that the various modes of operation include a mode "deactivated" (36) in which the integrated circuit (10) does not execute arithmetic operations.

6. A data processing device (100), notably a chip card, which is specifically intended to carry out a method as claimed in at least one of the preceding Claims and includes an integrated circuit (10) which executes useful arithmetic operations, notably cryptographic operations, in dependence on the first clock signal (18), characterized in that the device is provided with a clock control unit (14) which is connected to the integrated

circuit (10) as well as with a random generator (12) which is connected to the clock control unit (14), the clock control unit (14) being constructed in such a manner that it generates a second clock signal (20) in dependence on the random generator (12) and the first clock signal (18), which second clock signal varies at random and controls the integrated circuit (10).

7. A data processing device (100) as claimed in Claim 6, characterized in that the clock control unit (14) is constructed in such a manner that it switches, (via control leads 28) and in dependence on the random generator (12), the integrated circuit (10) to various modes of operation (30, 32, 34, 36) on a random basis.

8. A data processing device (100) as claimed in Claim 7, characterized in that the various modes of operation (30, 32, 34, 36) include at least two calculation methods (30, 34) which produce an identical result while using different arithmetical approaches.

9. A data processing device (100) as claimed in one of the Claims 7 or 8, characterized in that, the various modes of operation (30, 32, 34, 36) include at least one mode of operation "dummy" (32) in which the integrated circuit (10) does not execute useful operations but dummy arithmetic operations which act on predetermined or random input data, the result not being taken up in results or input data for the useful arithmetic operations.

10. A data processing device (100) as claimed in one of the Claims 7 to 9, characterized in that the various modes of operation (30, 32, 34, 36) include a mode "deactivated" (36) in which the integrated circuit (10) does not execute arithmetic operations.

11. A data processing device (100) as claimed in one of the Claims 7 to 10, characterized in that in at least one further mode of operation the time base (16) is additionally distorted so that the summing according to the "Differential Power Analysis" method is additionally impeded or made impossible.

LIST OF REFERENCES

100	data processing device
10	integrated circuit
12	random generator
14	clock control unit
16	horizontal axis t
18	signal $TAKT_1$
19	lead
20	signal $TAKT_2$
21	lead
22	signal DUMMY
24	signal DEAKT
26	signal ALT
28	control leads
29	line with modes of operation
30	mode of operation "method 1"
32	mode of operation "dummy"
34	mode of operation "method 2"
36	mode of operation "deactivated"
38	lead

ABSTRACT:

The present invention relates to a data processing device (100) as well as to a method of operating a data processing device, notably a chip card, which includes an integrated circuit (10) which executes useful arithmetic operations, notably cryptographic operations, in dependence on a first clock signal. Under random control a second clock signal is derived from the first clock signal so as to be applied to the integrated circuit (10) instead of the first clock signal while distances between clock edges of the second clock signal vary at random in time. To this end, there is provided a clock control unit (14) which is connected to the integrated circuit (10) as well as a random generator (12) which is connected to the clock control unit (14), the clock control unit (14) being constructed in such a manner that it generates a second clock signal (20) in dependence on the random generator (12) and the first clock signal (18), which second clock signal varies at random and controls the integrated circuit (10).

(Fig. 1)

Fig.1

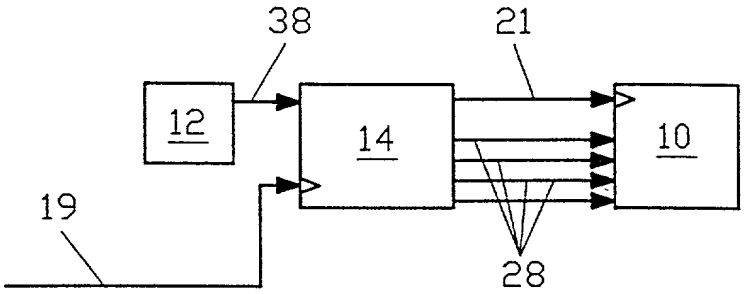
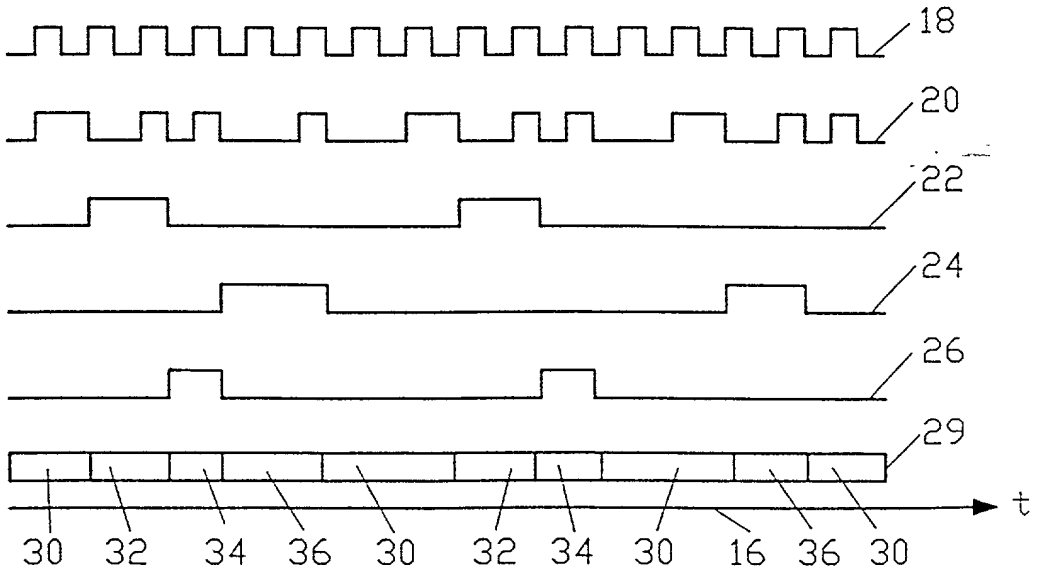


Fig.2



09/555303
526 Rec'd PCT/PTO 26 MAY 2000

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY
(includes Reference to PCT International Applications)

ATTORNEY'S DOCKET NUMBER
PHD 99.096 US

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which aa patent is sought on the invention entitled: "Data processing device and operating method for preventing a differential current consumption analysis"
the specification of which (check only one item below):
☐ is attached hereto.

☐ was filed as United States application

Serial No _____

on _____

and was amended

on _____

☒ was filed as PCT international application

Number PCT/EP99/07025

on 21 September 1999 (21.09.99)

and was amended under PCT Article 19

on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 USC 119
Germany	**19844962.3**	**30 September 1998**	**YES**
Germany	**19936938.0**	**5 August 1999**	**YES**

Combined Declaration For Patent Application and Power of Attorney (Continued) (includes Reference to PCT International Applications)	Attorneys Docket Number **PHD 99.096 US**

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) abnd/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (List name and registration number)

Algy Tamoshunas Reg. No. 27,677 Jack E. Haken, Reg. No. 26,902	Direct Telephone Calls to: (name and telephone number) (914)332-0222

201	FULL NAME OF INVENTOR	FAMILY NAME **FEUSER**	FIRST GIVEN NAME **Markus**	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY **Buchholz**	STATE OR FOREIGN COUNTRY **Germany** DE X	COUNTRY OF CITIZENSHIP **Germany**
	POST OFFICE ADDRESS	POST OFFICE ADDRESS **Hamburger Str. 4c**	CITY **21244 Buchholz**	STATE & ZIP CODE/COUNTRY **Germany**
202	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
203	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
204	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
205	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
206	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECONDE GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true: and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 if Title 18 of the United states Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
Markus Feuser		
DATE April 20, 2000	DATE	DATE
SIGNATURE OF INVENTOR 204	SIGNATURE OF INVENTOR 205	SIGNATURE OF INVENTOR 206
DATE	DATE	DATE